AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for generating a report on an unsolicited electronic message, comprising:

receiving an electronic mail message;

determining whether the electronic message is an unsolicited message;

if the message is an unsolicited message,

examining the message to identify a network address relating to the message,

identifying an authority hosting the network address,

generating a report containing the identified network address and hosting authority, and

transmitting the report to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected;

wherein identifying the hosting authority comprises identifying an owner of a network domain;

wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority.

2. (Original) The method of claim 1 further comprising transmitting the generated report to the identified hosting authority.

3. (Original) The method of claim 1 wherein examining the message to identify a network address comprises identifying a URL.

4. (Original) The method of claim 3 wherein identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL.

5. (Original) The method of claim 3 further comprising comparing the identified URL to a database of legitimate URLs.

6. (Original) The method of claim 5 further comprising updating the database based on electronic messages received.

7. (Original) The method of claim 3 wherein identifying the hosting authority comprises utilizing an Internet tool to locate a web server hosting the URL.

8. (Original) The method of claim 7 wherein utilizing an Internet tool comprises utilizing WHOIS.

9. (Cancelled)

10. (Original) The method of claim 1 wherein identifying the hosting authority comprises identifying an Internet service provider.

11. (Previously Presented) The method of claim 1 wherein the central managed service provider is configured to forward the report to the identified hosting authority.

12. (Original) The method of claim 1 further comprising at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period.

13. (Currently Amended) A system ~~for generating a report on an unsolicited electronic message~~, the system comprising:

a detector that detects a network address within an electronic message identified as an unsolicited message;

a host identifier that identifies an authority hosting the network address;

a report generator that generates a report containing the identified network address and hosting authority; and

a tangible computer readable storage medium that at least temporarily stores the identified network address and hosting authority;

wherein identifying the hosting authority comprises identifying an owner of a network domain;

wherein the system is operable such that the report is transmitted to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected;

wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority.

14. (Original) The system of claim 13 further comprising a detector operable to detect unsolicited messages.

15. (Original) The system of claim 13 wherein the network address is a URL.

16. (Original) The system of claim 13 wherein the hosting authority is an Internet service provider.

17. (Original) The system of claim 13 further comprising a processor operable to transmit the generated report.

18. (Original) The system of claim 17 wherein the processor is configured to transmit the report to the identified hosting authority.

19. (Previously Presented) The system of claim 17 wherein the processor is configured to transmit the report to the central managed service provider.

20. (Original) The system of claim 13 further comprising a database containing search terms used to identify the network address within text of the electronic message.

21. (Original) The system of claim 13 further comprising a database containing a list of trusted network addresses.

22. (Currently Amended) A computer product embodied on a tangible computer readable storage medium ~~for generating a report on an unsolicited electronic message~~, comprising:

code that receives an electronic mail message;

code that determines whether the electronic message is an unsolicited message;

code that examines the message to identify a network address relating to the message if the message is an unsolicited message[[,]];

code that identifies an authority hosting the network address;

code that generates a report containing the identified network address; and

a computer readable medium that stores said computer codes;

wherein identifying the hosting authority comprises identifying an owner of a network domain;

wherein the computer product is operable such that the report is transmitted to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected;

wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority.

23. (Currently Amended) The computer product of claim 22 wherein the computer readable medium ~~is selected from the group consisting~~includes at least one of CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive.

24. (Original) The computer product of claim 22 further comprising code that transmits the generated report to the identified hosting authority.

25. (Original) The computer product of claim 22 further comprising code that compares text within the electronic message to a database of words to locate the network address within the text.

26. (Original) The computer product of claim 22 further comprising code that compares the identified network address with trusted network addresses.

27. (Previously Presented) The method of claim 1 wherein identifying the hosting authority further comprises identifying an address, an administrative contact name, an administrative contact telephone number, and a name of at least one server associated with the hosting authority.

28. (Previously Presented) The method of claim 1 wherein identifying the hosting authority further comprises identifying an organization to which the network domain is registered.

29. (Previously Presented) The method of claim 28 wherein the report is utilized to generate an electronic mail message to be sent to the identified organization.

30. (Previously Presented) The method of claim 4, wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages.

31. (Previously Presented) The method of claim 1 wherein the report includes disclaimer information and user definable text.

32. (New) The method of claim 1, wherein the hosting authority message that the central managed service provider transmits to the hosting authority includes a hosting

authority report that includes a content of the message, a date and time the message arrived on a recipient's server, an IP address and name reported during an SMTP connection associated with the message, and a full WHOIS report used to track down the hosting authority.

33. (New) The method of claim 1, wherein the hosting authority message that the central managed service provider transmits to the hosting authority is signed to verify the central managed service provider as a source of the hosting authority message.